CVE-2023-6546

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-6546
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-21 20:15:00 UTC
Updated	2024-04-03 00:15:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	39	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	6.5	rc1	All	All
Operating System	Linux	Linux Kernel	6.5	rc2	All	All
Operating System	Linux	Linux Kernel	6.5	rc3	All	All
Operating System	Linux	Linux Kernel	6.5	rc4	All	All
Operating System	Linux	Linux Kernel	6.5	rc5	All	All
Operating System	Linux	Linux Kernel	6.5	rc6	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link	Tags
RHSA-2024:1607		access.redhat.com	
RHSA-2024:1018		access.redhat.com	
RHSA-2024:1614		access.redhat.com	
RHSA-2024:0930		access.redhat.com	
RHSA-2024:1612		access.redhat.com	

RHSA-2024:1612		access.redhat.com	
www.zerodayinitiative.com/advisories/ZDI-CAN-20527		www.zerodayinitiative.com	
RHSA-2024:1250		access.redhat.com	
access.redhat.com/security/cve/CVE-2023-6546		access.redhat.com	
RHSA-2024:1019		access.redhat.com	
RHSA-2024:0937		access.redhat.com	
RHSA-2024:1055		access.redhat.com	
RHSA-2024:1253		access.redhat.com	
RHSA-2024:1306		access.redhat.com	
github.com/torvalds/linux/commit/3c4f8333b582487a2d1e02171f1465531cde53e3		github.com	
RHBZ#2255498		bugzilla.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 161479 Oracle Enterprise Linux Security Update for kernel (ELSA-2024-1607)
- 242941 Red Hat Update for kernel (RHSA-2024:0930)
- 242942 Red Hat Update for kpatch-patch (RHSA-2024:0937)
- 242985 Red Hat Update for kernel (RHSA-2024:1018)
- 242986 Red Hat Update for kernel-rt (RHSA-2024:1019)
- 242994 Red Hat Update for kpatch-patch (RHSA-2024:1055)
- 243050 Red Hat Update for kernel (RHSA-2024:1250)
- 243053 Red Hat Update for kernel live patch module (RHSA-2024:1253)
- 243062 Red Hat Update for kernel-rt (RHSA-2024:1306)
- 243160 Red Hat Update for kernel security (RHSA-2024:1607)
- 243163 Red Hat Update for kpatch-patch (RHSA-2024:1612)
- 243167 Red Hat Update for kernel-rt (RHSA-2024:1614)
- 357089 Amazon Linux Security Advisory for kernel : ALAS2-2024-2443
- 673321 EulerOS Security Update for kernel (EulerOS-SA-2024-1337)
- 673547 EulerOS Security Update for kernel (EulerOS-SA-2024-1315)

673714 EulerOS Security Update for kernel (EulerOS-SA-2024-1196)

673723 EulerOS Security Update for kernel (EulerOS-SA-2024-1237)

673902 EulerOS Security Update for kernel (EulerOS-SA-2024-1176)

673992 EulerOS Security Update for kernel (EulerOS-SA-2024-1215)

673995 EulerOS Security Update for kernel (EulerOS-SA-2024-1275)

755604 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0129-1)

755607 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0115-1)

907788 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (32284)

907967 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (32284-1)

941650 AlmaLinux Security Update for kernel (ALSA-2024:1607)

961147 Rocky Linux Security Update for kernel (RLSA-2024:1607)

961150 Rocky Linux Security Update for kernel-rt (RLSA-2024:1614)

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**